

1 **USER AUTHENTICATION METHOD, AND STORAGE MEDIUM,**
2 **APPARATUS AND SYSTEM THEREFOR**

3 Abstract

4 The invention provides a user authentication method and
5 apparatus whereby, even when multiple verifiers
6 correspond with a prover, safe user authentication is
7 ensured while zero knowledge property is acquired. In
8 an example embodiment, at step 1, a prover calculates A
9 $= F(g, a)$ using a random number a , and transmits A to a
10 verifier (process Ps1, communication T1). At step 2,
11 the verifier uses a random number b to calculate
12 cryptograms $B = F(g, b)$ and $X = F(A, b)$, and transmits B
13 and X to the prover (process Qs1, communication T2). At
14 step 3, the prover determines whether $X = F(B, a)$ has
15 been established. If $X = F(B, a)$ has not been
16 established, the prover halts performance of the
17 protocol procedures. If $X = F(B, a)$ has been
18 established, the prover 10 uses a random number c to
19 calculate $C = F(g, c)$ and $Y = F(B, c)$ and thereafter
20 calculates $Z = H(a, Y, s)$, and then transmits C , Y and Z
21 to the verifier 40 (process Ps2, communication T3). At
22 step 4, the verifier determines whether $Y = F(C, b)$ and
23 $A = J(v, Y, g, Z)$ have been established. If $Y = F(C, b)$
24 and $A = J(v, Y, g, Z)$ have been established, the
25 verifier 40 accepts the identity of the prover 10. If Y
26 $= F(C, b)$ and $A = J(v, Y, g, Z)$ have not been
27 established, the verifier rejects the identity of the
28 prover (process Qs2).